

# EUROPEAN PATENT OFFICE

## Patent Abstracts of Japan

PUBLICATION NUMBER : 11143780  
PUBLICATION DATE : 28-05-99

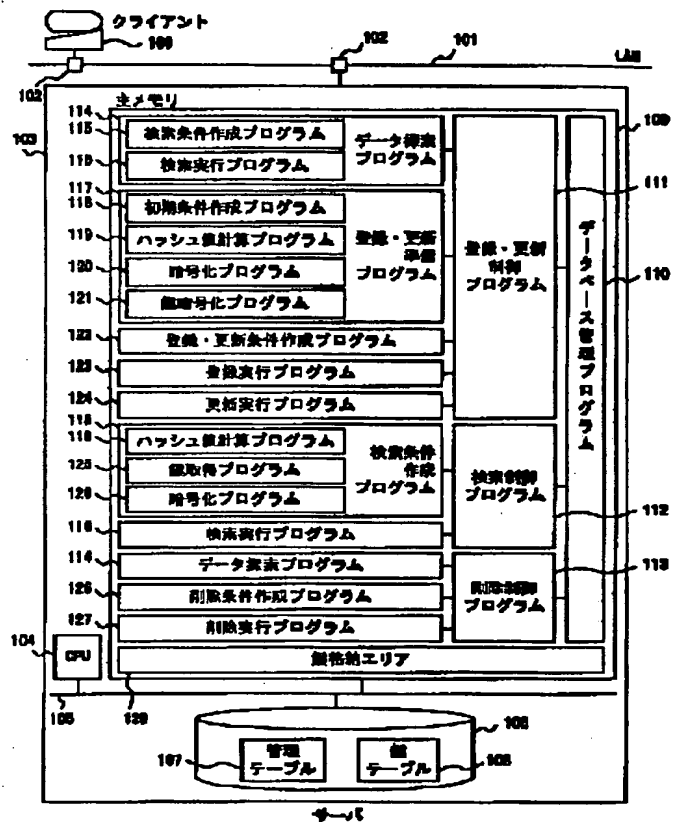
APPLICATION DATE : 05-11-97  
APPLICATION NUMBER : 09319010

APPLICANT : HITACHI LTD;

INVENTOR : MATSUNAGA KAZUO;

INT.CL. : G06F 12/14 G06F 12/00 G06F 17/30  
G09C 1/00 G09C 1/00

TITLE : METHOD AND DEVICE FOR  
MANAGING SECRET INFORMATION IN  
DATABASE



ABSTRACT : PROBLEM TO BE SOLVED: To improve the flexibility and stability of and database to be enciphered by managing information related with encipherment through the use of an exclusive table.

SOLUTION: Encipherment data are managed by a management table 107 of a database to be enciphered and a key table 108 corresponding to the table. The key table 108 has a cryptographic key, an encipherment algorithm identifier, and a data hash value for each group of specific values (the item, line, and column of one column in one line). At each time of the registration or update of data for the management table 107, the cryptographic key is generated by a data encipherment program 112, and the cryptographic key is enciphered by using a key cryptographic key, and registered in the key table 108. Retrieval of the enciphered data is operated by deciphering the cryptographic key obtained by the hash value by using the key cryptographic key, and using the deciphered cryptographic key and the encipherment algorithm. Thus, change of the cryptographic key or the encipherment algorithm can be attained during database activation.

COPYRIGHT: (C)1999,JPO

**This Page Blank (uspto)**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-143780

(43) 公開日 平成11年(1999) 5月28日

(51) Int.Cl.<sup>8</sup>

識別記号

F I

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 B

12/00

5 3 7

12/00

5 3 7 H

17/30

G 0 9 C 1/00

6 3 0 A

G 0 9 C 1/00

6 3 0

6 6 0 D

6 6 0

G 0 6 F 15/40

3 2 0 A

審査請求 未請求 請求項の数10 F D (全 22 頁)

(21) 出願番号

特願平9-319010

(22) 出願日

平成9年(1997)11月5日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 茶谷 謙一

神奈川県川崎市幸区鹿島田890番地 株式

会社日立製作所情報・通信開発本部内

(72) 発明者 北川 誠

神奈川県川崎市幸区鹿島田890番地 株式

会社日立製作所情報・通信開発本部内

(72) 発明者 松永 和男

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

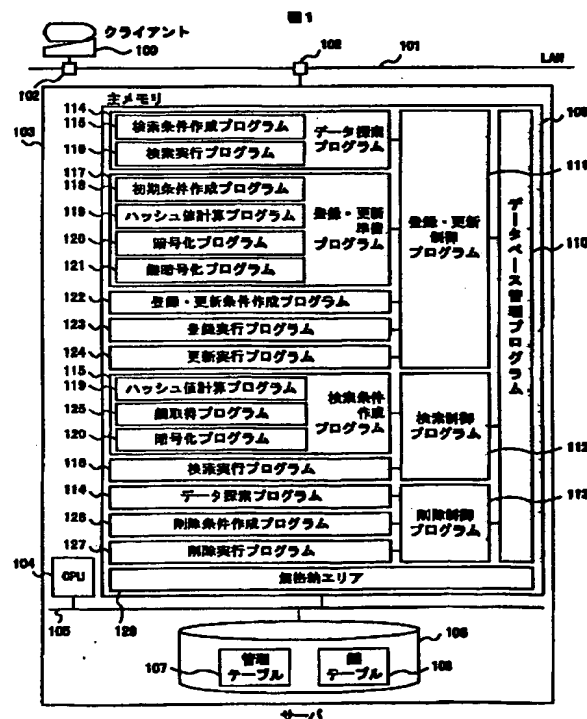
(74) 代理人 弁理士 笹岡 茂 (外1名)

(54) 【発明の名称】 データベースにおける秘密情報管理方法およびデータベースの秘密情報管理装置

(57) 【要約】

【課題】 暗号化に関する情報を専用のテーブルを使って管理することにより、暗号化するデータベースの柔軟性と安全性を向上する。

【解決手段】 暗号化するデータベースの管理テーブル107とそのテーブルに対応する鍵テーブル108により、暗号化データを管理する。鍵テーブル108は特定の値の集合(1つの行の中の1つの列の項目、行、列)ごとに暗号鍵、暗号化アルゴリズム識別子、データのハッシュ値を持つ。管理テーブル107へのデータの登録または更新ごとにデータ暗号化プログラム112において暗号鍵を作成し、さらに該暗号鍵を鍵暗号鍵を用いて暗号化し、これを鍵テーブル108に登録する。暗号データの検索は、ハッシュ値によって得られる暗号鍵を鍵暗号鍵を用いて復号し、復号した暗号鍵と暗号化アルゴリズムを用いて行う。これによりデータベース稼動中に暗号鍵や暗号化アルゴリズムの変更を可能にする。



**【特許請求の範囲】**

【請求項1】 暗号化された秘密情報を管理するデータベースにおける秘密情報管理方法であって、前記データベースに、暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（1つの行の中の1つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを設け、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けし、前記データベースへの秘密情報の登録時に、シリアル番号を作成し、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録し、前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化し、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算し、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録することを特徴とするデータベースにおける秘密情報管理方法。

【請求項2】 請求項1記載の秘密情報管理方法において、前記データベースに登録された秘密情報の検索時に、検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出し、該条件一致行から前記鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出し、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号し、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行うことを特徴とするデータベースにおける秘密情報管理方法。

【請求項3】 請求項2記載のデータベースにおける秘密情報管理方法において、検索条件に一致する秘密情報を検索後に、該検索した秘密情報を暗号化するための新たな鍵を乱数を使って作成し、該作成した鍵により該検索した秘密情報を暗号アルゴリズムを用いて新たに暗号化し、該作成した鍵を前記鍵暗号鍵により暗号化し、該新たに暗号化した秘密情報で管理テーブルを更新し、前記鍵暗号鍵により暗号化した暗号化のための新たな鍵と前記暗号アルゴリズムの識別子により鍵テーブルを更新することを特

徴とするデータベースにおける秘密情報管理方法。

【請求項4】 請求項2記載のデータベースにおける秘密情報管理方法において、前記データベースに登録された秘密情報の更新時に、更新前の秘密情報と更新後の秘密情報を入力し、更新前の秘密情報によりデータベースを検索し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得し、前記更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録し、前記作成した鍵を前記鍵暗号鍵により暗号化し、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録することを特徴とするデータベースにおける秘密情報管理方法。

【請求項5】 暗号化された秘密情報を管理するデータベースの秘密情報管理装置であって、前記データベースに、暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（1つの行の中の1つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けし、秘密情報の登録時にシリアル番号を作成する手段と、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化する手段と、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録する手段と、前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化する手段と、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算する手段と、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録する手段と、秘密情報の検索時に検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出す手段と、該条件一致行から前記鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出す手段と、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号する

手段と、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行う手段を備えることを特徴とするデータベースの秘密情報管理装置。

【請求項6】 請求項5記載のデータベースの秘密情報管理装置において、

秘密情報の更新時に、入力された更新前の秘密情報によりデータベースを検索し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得する手段と、入力された更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化する手段と、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録する手段と、前記作成した鍵を前記鍵暗号鍵により暗号化する手段と、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録する手段を備えることを特徴とするデータベースにおけるデータベースの秘密情報管理装置。

【請求項7】 暗号化された秘密情報と暗号化に用いた鍵情報を記録したコンピュータ読み取り可能な記録媒体であって、

前記暗号化された秘密情報は管理テーブルに登録され、前記暗号化に用いた鍵情報は鍵テーブルに登録され、前記管理テーブルは、複数の行と複数の列からなり、各行対応に暗号化された秘密情報の組が記録され、前記鍵テーブルは、複数の行と複数の列からなり、前記管理テーブルの特定の値の集合（1つの行の中の1つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値が記録され、前記管理テーブルと鍵テーブルの各行には管理テーブルの行と鍵テーブルの行を互に関連付けるシリアル番号が記録されたことを特徴とする暗号化された秘密情報と暗号化に用いた鍵情報を記録したコンピュータ読み取り可能な記録媒体。

【請求項8】 暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（1つの行の中の1つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互に関連付けしたデータベースを管理する秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記データベースへの秘密情報の登録時にシリアル番号を作成する手段と、登録する秘密情報を暗号化するため

の鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化する手段と、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録する手段と、前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化する手段と、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算する手段と、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録する手段を実行させる秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項9】 暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（1つの行の中の1つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互に関連付けしたデータベースを管理する秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記データベースへの秘密情報の検索時に検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出す手段と、該条件一致行から、秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出す手段と、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号する手段と、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行う手段を実行させる秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項10】 暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（1つの行の中の1つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互に関連付けしたデータベースを管理する秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記データベースに登録された秘密情報の更新時に、入力された更新前の秘密情報によりデータベースを検索

し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得する手順と、入力された更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化する手順と、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録する手順と、前記作成した鍵を秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化する手順と、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録する手順を実行させる秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、秘密情報をデータベースに暗号化して登録し、管理する方法に関するものである。

##### 【0002】

【従来の技術】昨今、データベースは、クレジット会社、銀行など様々な分野で利用されている。特に最近では、電子商取引の認証を行う認証局も、認証のために氏名やクレジット番号などの個人の秘密情報を管理するデータベースを持っている。このようなデータベースは個人に関する秘密情報を扱っているため、例えばデータベースを操作できるアクセス権をデータベース管理者のような特定の個人にしか与えないようにすることにより、データの漏洩を防いでいる。しかしながら、データベースへのアクセス権を設定している場合でも、不正な侵入者がデータベースを記録した記憶装置を不正に持ち出し、該装置の内容を直接見ることでデータが漏洩する危険性がある。そこで、氏名やクレジット番号など特定の情報を暗号化して登録し、情報を取り出すときに復号して元の情報を得ることによりセキュリティを確保することが考えられる。このように特定の情報を暗号化しておくことにより、データベースが記録された装置が盗難にあったとしても復号のための鍵が盗まれていなければ、情報が漏洩する危険性は大幅に減少する。従来は、このような情報の暗号化に特定の一つの鍵を用いて、データベース全体を暗号化していた。

【0003】データベースを暗号化する技術の例としては「特開平8-329011」に開示されているものがある。該公知例の実施例は、データベース、鍵管理センタ、1次ユーザ、2次ユーザを相互に接続するネットワークシステムから構成される。1次ユーザは著作権情報を暗号化してデータベースに格納し、鍵を鍵管理センタに格納する。2次ユーザがその著作権情報を利用するときは、鍵管理センタから暗号鍵をもらい、そのときに課金される方式が提案されている。この公知例の鍵管理センタは、保管されている鍵と著作権ラベルの対応づけを

行うことによって鍵を管理している。

##### 【0004】

【発明が解決しようとする課題】従来の技術では、特定の一つの暗号鍵でデータベース全体を暗号化したデータベースでは、その暗号鍵がデータベースが記録された装置と同時に盗難にあった場合、データベース全体が解読され、秘密情報が漏洩する危険性がある。また、データベースの稼働中に暗号鍵が盗難にあった場合、不正侵入者がこの鍵を使用してデータを解読する可能性がある。従って、これらの状況においては暗号鍵を変更してデータの漏洩を防止する必要がある。暗号鍵を変更するためには、データベースに対するユーザからのアクセスを禁止し、データベース中のすべてのデータを一旦復号化した後で新しい暗号鍵で暗号化し直さなければならない。データベースの規模が大きくなればなるほどこの作業には時間がかかり、その間、ユーザはデータベースにアクセスできない。さらに鍵が盗難に会わなくとも、暗号化されたデータのうち一つが解読されると、データベースを暗号化している鍵が一つであるため、他のデータがすべて解読される危険性がある。

【0005】また、従来の技術ではデータベースの稼働中に、より強固な暗号化アルゴリズムを採用してセキュリティを高めようとする場合に、暗号化アルゴリズムを変更することが困難である。なぜなら、この場合にもデータベースへのユーザアクセスを一旦禁止し、すべてのデータを新しい暗号化アルゴリズムで暗号化し直さなければならないからである。以上で述べたように、従来のデータベースを暗号化する方式においては、データベースを暗号化する鍵が1つであるためその鍵が盗難に合った場合、その鍵で暗号化されたデータベースがすべて解読され秘密情報が漏洩する危険性があり、また暗号化したデータベース稼働中により強固な暗号化アルゴリズムが発明されたとしてもデータベースの暗号化アルゴリズムをその方式に変更するのは困難であるという問題があった。

【0006】本発明は、データベースを暗号化する方式において、データベースの内容を漏洩しない安全なデータベースの秘密情報管理方式を提供すること、暗号鍵や暗号化アルゴリズムの変更をデータベース稼働中にも容易に行うことができるようにすること、および複数の暗号化アルゴリズムと複数の暗号鍵を使うことができるようにすることを目的とする。

##### 【0007】

【課題を解決するための手段】上記目的を達成するため、本発明は、暗号化された秘密情報を管理するデータベースにおける秘密情報管理方法であって、前記データベースに、暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（1つの行の中の1つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム

識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを設け、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互に関連付けし、前記データベースへの秘密情報の登録時に、シリアル番号を作成し、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録し、前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化し、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算し、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録するようにしている。

【0008】また、前記データベースに登録された秘密情報の検索時に、検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出し、該条件一致行から前記鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出し、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号し、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行うようにしている。

【0009】また、検索条件に一致する秘密情報を検索後に、該検索した秘密情報を暗号化するための新たな鍵を乱数を使って作成し、該作成した鍵により該検索した秘密情報を暗号アルゴリズムを用いて新たに暗号化し、該作成した鍵を前記鍵暗号鍵により暗号化し、該新たに暗号化した秘密情報で管理テーブルを更新し、前記鍵暗号鍵により暗号化した暗号化のための新たな鍵と前記暗号アルゴリズムの識別子により鍵テーブルを更新するようにしている。

【0010】また、前記データベースに登録された秘密情報の更新時に、更新前の秘密情報と更新後の秘密情報を入力し、更新前の秘密情報によりデータベースを検索し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得し、前記更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録し、前記作成した鍵を前記鍵暗号鍵により暗号化し、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録す

るようにしている。

【0011】

【発明の実施の形態】まず、本発明の原理について説明する。秘密情報を管理するデータベースは、暗号化された秘密情報を格納するための管理テーブルと、その管理テーブルの1つの行の中の1つの列の項目（以下では、フィールドと称する）、行、または列などの特定の値の集合ごとに該集合に属する個々の値を暗号化するために使用した鍵と暗号アルゴリズム識別子を格納する鍵テーブルを有する。前記管理テーブルと鍵テーブルは、2つのテーブルの行を関連付けるシリアル番号をそれぞれ格納しており、前記管理テーブルの特定の値の集合を結合した値に対して計算したハッシュ値も鍵テーブルに格納する。暗号化した秘密情報の登録には、まず、秘密情報を暗号化するための鍵（以下では、データ暗号鍵と称する）を乱数を使って作成する。そのデータ暗号鍵を使って管理テーブルに登録する秘密情報を暗号化する。このような鍵の例としてMULTI2、DES(Data Encryption Standard)等がある。さらに、前記データ暗号鍵は、秘密情報を暗号化する鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する別の鍵（以下では、鍵暗号鍵と称する）を用いて暗号化される。そして、秘密情報の検索のために使用するハッシュ値を暗号化前の秘密情報から計算する。さらに、シリアル番号を生成し、シリアル番号と暗号化された秘密情報を管理テーブルに登録し、シリアル番号とデータ暗号鍵と暗号化アルゴリズム識別子とハッシュ値を鍵テーブルに登録する。

【0012】検索条件としてシリアル番号が指定された場合は、鍵テーブルにおいてそのシリアル番号を検索し、鍵テーブルからそのシリアル番号に一致する暗号化アルゴリズム識別子と暗号化されたデータ暗号鍵を取り出し、鍵暗号鍵で暗号化されたデータ暗号鍵を復号する。次に管理テーブルにおいてシリアル番号を検索し、管理テーブルから、シリアル番号に一致する暗号化された秘密情報を取り出し、その秘密情報を前記暗号アルゴリズムで前記データ暗号鍵を使って復号する。検索条件として秘密情報のみが指定された場合は、まず、検索条件のハッシュ値を計算する。そのハッシュ値により鍵テーブルを検索してそのハッシュ値に一致する暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子をすべて取り出し、前記暗号化されたデータ暗号鍵を復号したデータ暗号鍵と、暗号化アルゴリズムにより検索条件を暗号化する。次に、暗号化した検索条件を使って管理テーブルを検索し、一致する秘密情報を含む行が見つかった場合、その行のシリアル番号に対応する鍵テーブルの他の暗号化されたデータ暗号鍵を復号した鍵と暗号化アルゴリズム識別子を使って、検索条件以外の秘密情報を復号する。

【0013】以上説明した原理を、さらに具体例を用いて説明する。本例で用いる管理テーブルの例を図2に示し、その管理テーブルに対応する鍵テーブルを図3に示す。管理テーブルの列は、シリアル番号、名前、電話番号、住所で構成され、鍵テーブルの列は、シリアル番号、名前のハッシュ値、名前暗号化アルゴリズム識別子、名前の暗号鍵、電話番号のハッシュ値、電話番号暗号化アルゴリズム識別子、電話番号の暗号鍵、住所のハッシュ値、住所暗号化アルゴリズム識別子、住所の暗号鍵で構成される。図2、図3において、天地逆の文字は暗号化されているデータを示している。図2の管理テーブルには、名前、電話番号が暗号化され、住所が暗号化されないで格納されている。図3の鍵テーブルには、名前、電話番号、住所のそれぞれのハッシュ値、暗号化アルゴリズム識別子、暗号鍵が格納され、このうち暗号鍵は暗号化されて格納されている。

【0014】本例で、シリアル番号の項目200の列が「11」の行204と、シリアル番号の項目200の列が「12」の行205が、管理テーブルに格納されており、シリアル番号の項目300の列が「11」の行310と、シリアル番号の項目300の列が「12」の行311が、鍵テーブル108に格納されている状態で、新たに名前「日立花子」、電話番号「987-6543」、住所「東京都」をデータベースに登録する場合の手順について説明する。まず、「日立花子」、「987-6543」を暗号化するための鍵を乱数を使ってそれぞれ作成し、「315TK8」「123ABD」を求める。次に作成した鍵「315TK8」を使って「日立花子」を暗号化プログラムが持つ最新の暗号化アルゴリズムで暗号化し、鍵「123ABD」を使って「987-6543」を前記暗号化アルゴリズムで暗号化する。次に「日立花子」からハッシュ値「502」を計算し、「987-6543」からハッシュ値「143」を計算し、「東京都」からハッシュ値「123」を計算する。鍵「315TK8」、「123ABD」を鍵暗号鍵で暗号化する。管理テーブルと鍵テーブルの行を関係付けるシリアル番号「13」を生成し、管理テーブルのシリアル番号の項目207に「13」、名前の項目208に暗号化された「日立花子」、電話番号の項目209に暗号化された「987-6543」、住所の項目210に「東京都」を登録し、鍵テーブルのシリアル番号の項目312に「13」、名前のハッシュ値の項目313に「502」、名前の暗号化アルゴリズム識別子の項目314に「2」、名前の暗号鍵の項目315に暗号化された「315TK8」、電話番号のハッシュ値の項目316に「143」、電話番号の暗号化アルゴリズム識別子の項目317に「2」、電話番号の暗号鍵の項目318に暗号化された「123ABD」、住所のハッシュ値の項目319に「123」、住所の暗号化アルゴリズム識別子の項目320に「0」を登録する。

【0015】次に、この秘密情報データベース（管理テーブルと鍵テーブル）から、名前が「日立二郎」の電話番号を検索する場合について説明する。まず、「日立二郎」からハッシュ値を計算し、ハッシュ値「359」を求める。鍵テーブルの名前のハッシュ値で「359」を検索して、その暗号化アルゴリズム識別子「1」322と暗号化されたデータ暗号鍵「ZXB515」323を取り出す。次にデータ暗号鍵を鍵暗号鍵で復号する。復号した暗号鍵「ZXB515」323と暗号化アルゴリズム識別子「1」322を使って名前の検索条件「日立二郎」を暗号化する。暗号化された「日立二郎」の検索条件を使って管理テーブルを検索する。管理テーブルにおいて暗号化された「日立二郎」を検索し、その行のシリアル番号「12」211を取り出し、そのシリアル番号「12」211を使って鍵テーブルの電話番号の暗号化アルゴリズム識別子「1」324と暗号化されたデータ暗号鍵「01ER88」を鍵暗号鍵で復号した鍵を使って管理テーブル上の「日立二郎」の暗号化された電話番号を復号化する。

【0016】次に、各行に含まれる値のそれぞれに同一のデータ暗号鍵を使用し、かつ各行ごとに異なるデータ暗号鍵を使用する場合について説明する。この場合の管理テーブルと鍵テーブルの例を図4、図5に示す。図4は、行ごとに暗号化された管理テーブルの例である。図4のテーブル構成は図2と同じであるが、暗号化されて格納されている単位が図2と異なり、行ごとになっている。図4において、天地逆の文字は暗号化されているデータを示している。図4の管理テーブルに対応する鍵テーブルの例を図5に示す。図5の鍵テーブルは、シリアル番号、名前と電話番号を連結した値のハッシュ値、暗号化アルゴリズム識別子、およびデータ暗号鍵を列に持つ。鍵テーブルは行ごとに暗号化した鍵を持つのでハッシュ値、暗号化アルゴリズム識別子、暗号鍵は行ごとに1つだけ存在する。図5において、天地逆の文字は暗号化されているデータを示している。シリアル番号の項目の列500は、管理テーブルと鍵テーブルの行を関連付けるためのシリアル番号を格納する。図5では、名前、電話番号の2つを組み合わせて計算されるハッシュ値を、名前、電話番号のハッシュ値の項目の列501に格納しているが、これは名前だけの1つからハッシュ値を計算するようにしてもよい。図4の管理テーブルと図5の鍵テーブルの構造を持つデータベースにより、行ごとにそれぞれ別のデータ暗号鍵で暗号化することが可能となる。

【0017】本例で、シリアル番号の項目の列400が「11」の行404と、シリアル番号の項目の列400が「12」の行405が、管理テーブルに格納されており、シリアル番号の項目の列500が「11」の行504と、シリアル番号の項目の列500が「12」の行505が、鍵テーブルに格納されている状態で、新たに名



前「日立花子」、電話番号「987-6543」、住所「東京都」をデータベースに登録する場合の手順について説明する。まず、「日立花子」、「987-6543」、「東京都」を暗号化するための鍵を乱数を使って1つ作成し、「315TK8」を求める。次に作成した鍵「315TK8」を使って「日立花子」、「987-6543」、「東京都」をそれぞれ暗号化プログラムが持つ最新の暗号アルゴリズムで暗号化する。次に「日立花子」、「987-6543」からハッシュ値「532」を計算する。鍵「315TK8」を鍵暗号鍵で暗号化する。管理テーブルと鍵テーブルの行を関係付けるシリアル番号「13」を生成し、管理テーブルのシリアル番号の項目407に「13」、名前の項目408に暗号化された「日立花子」、電話番号の項目409に暗号化された「987-6543」、住所の項目410に暗号化された「東京都」を登録し、鍵テーブルのシリアル番号の項目506に「13」、名前、電話番号のハッシュ値の項目507に「532」、暗号化アルゴリズム識別子の項目508に「1」、暗号鍵の項目509に暗号化された「315TK8」を登録する。

【0018】次に、この秘密情報データベース（管理テーブルと鍵テーブル）から、名前が「日立二郎」で電話番号が「123-4567」の住所を検索する場合について説明する。行ごとに暗号化されたデータベースにおいて暗号化された情報を検索する場合、ハッシュ値を計算するために使用した項目はすべて検索条件の中に指定しなければならない。まず、「日立二郎」、「123-4567」からハッシュを計算し、ハッシュ値「459」を求める。鍵テーブルの名前、電話番号のハッシュ値で「459」を検索して、その暗号化アルゴリズム識別子「1」512と暗号化されたデータ暗号鍵「PB24CS」513を取り出す。次にデータ暗号鍵を鍵暗号鍵で復号する。

【0019】取り出した暗号鍵「PB24CS」513と暗号化アルゴリズム識別子「1」512を使って「日立二郎」、「123-4567」を暗号化した検索条件を作成する。暗号化された「日立二郎」、「123-4567」の検索条件を使って管理テーブルを検索する。管理テーブルにおいて暗号化された「日立二郎」、「123-4567」を検索し、一致する行が管理テーブルにあれば、「日立二郎」、「123-4567」を暗号化した鍵と暗号化アルゴリズムを使って、シリアル番号が「12」の行の管理テーブルの暗号化された住所を復号化する。

【0020】暗号化する特定の集合が列の場合の管理テーブルと鍵テーブルの例を図6、図7に示す。図6のテーブル構成はシリアル番号の項目がない点が図2と異なる。図6において、天地逆の文字は暗号化されているデータを示している。図6では住所の項目602のデータは暗号化されないで格納されている。図6の管理テー

ブルに対応する鍵テーブルの例を図7に示す。図7において、天地逆の文字は暗号化されているデータを示している。図7は、各列に含まれる値のそれぞれに同一のデータ暗号鍵を使用し、かつ各列ごとに異なるデータ暗号鍵を使用する場合の鍵テーブルの例である。この場合は、列ごとにすべての行が同じ暗号鍵と暗号化アルゴリズムを使うので、ハッシュ値を格納しない。図6の管理テーブルと図7の鍵テーブルの構造を持つデータベースにより、列ごとにそれぞれ別の暗号鍵を持つデータベースの暗号化が可能となる。

【0021】本例で、管理テーブルの行603と行604が、管理テーブルに格納されており、行711が、鍵テーブルに格納されている状態で、新たに名前「日立花子」、電話番号「987-6543」、住所「東京都」をデータベースに登録する場合の手順について説明する。まず、「日立花子」、「987-6543」を暗号化するための鍵を取得する。そのために鍵暗号鍵で暗号化された「24B52C」、「SW610V」と暗号化アルゴリズム識別子「1」、「1」を鍵テーブルから取得し、鍵暗号鍵で暗号化された「24B52C」、「SW610V」を鍵暗号鍵で復号する。次に取得した鍵「24B52C」を使って「日立花子」を鍵テーブルから取り出した暗号アルゴリズムで暗号化し、鍵「SW610V」を使って「987-6543」を前記暗号化アルゴリズムで暗号化する。

【0022】次に、この秘密情報データベース（管理テーブルと鍵テーブル）から、名前が「日立二郎」の電話番号を検索する場合について説明する。まず、鍵テーブルから名前の暗号化アルゴリズム識別子「1」706と暗号化されたデータ暗号鍵「24B52C」707を取り出す。次に暗号化されたデータ暗号鍵「24B52C」を鍵暗号鍵で復号する。前記データ暗号鍵「24B52C」707を暗号化アルゴリズム識別子「1」706を使って名前の検索条件「日立二郎」を暗号化する。暗号化された「日立二郎」の検索条件を使って管理テーブルを検索する。「日立二郎」の行の暗号化された電話番号を鍵テーブルの電話番号の暗号鍵「SW610V」709を復号化したものと暗号化アルゴリズム識別子「1」を使って復号化する。

【0023】以上のように、秘密情報を暗号化して登録するデータベースにおいて、暗号化した秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（1つの行の中の1つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号化アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルの2つを使って管理することにより、管理テーブルの特定の値の集合ごとに暗号鍵と暗号化アルゴリズムを変更することが可能となる。

【0024】以下、本発明の第一の実施例について図1

を用いて説明する。本システムは、クライアント100、LAN101、LANアダプタ102、サーバ103から構成される。クライアント100とサーバ103は、LANアダプタ102を介してLAN101により接続される。サーバ103は、CPU104、主メモリ109、バス105、磁気ディスク装置106から構成される。主メモリ109と磁気ディスク装置106は、CPU104よりバス105を介してアクセスされる。主メモリ109には、データベース管理プログラム110、登録・更新制御プログラム111、検索制御プログラム112、削除制御プログラム113、データ探索プログラム114、登録・更新準備プログラム117、登録・更新条件作成プログラム122、登録実行プログラム123、更新実行プログラム124、検索条件作成プログラム115、検索実行プログラム116、削除条件作成プログラム126、削除実行プログラム127および鍵格納エリア128が格納される。

【0025】データ探索プログラム114は、検索条件作成プログラム115と検索実行プログラム116で構成される。登録・更新準備プログラム117は、初期条件作成プログラム118、ハッシュ値計算プログラム119、暗号化プログラム120、および鍵暗号化プログラム121で構成される。検索条件作成プログラムは、ハッシュ値計算プログラム119、鍵取得プログラム125、および暗号化プログラム120で構成される。磁気ディスク装置106には、管理テーブル107と鍵テーブル108が格納される。

【0026】以下、図1の構成のシステムにおいて、データベースに暗号化して格納するデータの登録処理の概略について説明する。ユーザがクライアント100からデータベースに登録するデータを入力する。登録・更新制御プログラム111が起動され、クライアント100から入力された登録するデータが登録・更新制御プログラム111に渡される。登録・更新制御プログラム111は、登録・更新準備プログラム117に登録するデータを渡す。登録・更新準備プログラム117は、初期条件作成プログラム118によりシリアル番号を作成し、ハッシュ値計算プログラム119により登録するデータのハッシュを計算し、暗号化プログラム120により登録するデータを暗号化する鍵を作成して、暗号化プログラム120が持っている最新の暗号化アルゴリズムにより登録するデータを暗号化し、さらにその暗号化の鍵を鍵暗号化プログラム121が持っている暗号化アルゴリズムにより鍵格納エリア128にある鍵で暗号化する。登録・更新準備プログラム117は、シリアル番号、登録されるデータのハッシュ値、暗号化された登録データ、暗号化した登録データを暗号化した鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、シリアル番号、登録されるデータのハッシュ

値、暗号化された登録データ、暗号化した登録データを暗号化した鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録・更新条件作成プログラム122に渡す。登録・更新条件作成プログラム122は、渡されたデータから管理テーブル107と鍵テーブル108のためのSQL文をそれぞれ作成し、それを登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、登録・更新条件作成プログラム122で作成したSQL文を登録実行プログラム123に渡す。登録実行プログラム123は、データベース管理プログラム110を使って管理テーブル107に、シリアル番号、暗号化された登録データを登録し、鍵テーブル108に、シリアル番号、登録されるデータのハッシュ値、暗号化した登録データを暗号化した鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録する。

【0027】次に、このような構成の本システムにおいて、暗号化してデータベースに登録したデータの検索処理の概略について説明する。ユーザがクライアント100から検索するデータを入力する。検索制御プログラム112が起動され、クライアント100から入力された検索するデータが検索制御プログラム112に渡される。検索制御プログラム112が検索条件作成プログラム115に検索するデータを渡す。検索条件作成プログラム115は、ハッシュ値計算プログラム119により検索するデータのハッシュ値を計算し、鍵取得プログラム125により鍵テーブル108から前記ハッシュ値に一致する行の暗号化された暗号鍵と、暗号化アルゴリズム識別子を取り出す。暗号化されたデータ暗号鍵を鍵暗号鍵で復号する。復号したデータ暗号鍵と暗号化アルゴリズム識別子で検索条件を暗号化し、検索のためのSQL文を作成する。検索条件作成プログラム115は、作成したSQL文を検索制御プログラム112に渡す。検索制御プログラム112は、前記SQL文を検索実行プログラム116に渡す。検索実行プログラム116は、データベース管理プログラム110を使って暗号化された検索条件に一致するデータを管理テーブル107から検索する。データベース管理プログラム110は、検索結果を、検索制御プログラム112に渡す。検索制御プログラム112は、検索結果を復号してクライアント100に復号した検索結果を返す。クライアント100は、検索結果を画面に表示する。

【0028】次に、このような構成の本システムにおいて、暗号化してデータベースに格納したデータの更新処理の概略について説明する。ユーザがクライアント100から更新前のデータと更新後のデータを入力する。登録・更新制御プログラム111が起動され、クライアント100から入力された更新前データと更新後のデータが登録・更新制御プログラム111に渡される。登録・更新制御プログラム111は、更新前のデータをデータ探索プログラム114に渡す。データ探索プログラム1

14は、検索条件作成プログラム115により更新前のデータを暗号化し、検索実行プログラム116により更新前のデータのシリアル番号を取り出し、登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、シリアル番号、更新後のデータを登録・更新準備プログラム117に渡す。登録・更新準備プログラム117は、ハッシュ値計算プログラム119により、更新後のデータのハッシュ値を計算し、暗号化プログラム120により更新後のデータを暗号化する鍵を作成し、更新するデータを暗号化プログラム120が持っている最新の暗号化アルゴリズムで暗号化し、さらに鍵暗号化プログラム121が、その暗号化の鍵を鍵格納エリア128にある鍵暗号鍵で鍵暗号化プログラム121が持っている暗号化アルゴリズムにより暗号化する。

【0029】登録・更新準備プログラム117は、更新後のデータのハッシュ値、暗号化された更新後のデータ、暗号化された更新後のデータを暗号化した鍵、更新後のデータを暗号化した暗号化アルゴリズム識別子を登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、シリアル番号、更新後のデータのハッシュ値、暗号化された更新後のデータ、暗号化された更新後のデータを暗号化した鍵、更新後のデータを暗号化した暗号化アルゴリズム識別子を登録・更新条件作成プログラム122に渡す。登録・更新条件作成プログラム122は、渡されたデータから管理テーブル107と鍵テーブル108のためのSQL文をそれぞれ作成し、それを登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、登録・更新条件作成プログラム122で作成したSQL文を更新実行プログラム124に渡す。更新実行プログラム124は、データベース管理プログラム110を使って、管理テーブル107の暗号化された更新後のデータと鍵テーブル108の更新後のデータのハッシュ値、暗号化された更新後のデータを暗号化した鍵、暗号化アルゴリズム識別子をシリアル番号にしたがって更新する。

【0030】次に、このような構成の本システムにおいて、暗号化してデータベースに格納したデータの削除処理の概略について説明する。ユーザがクライアント100から削除するデータを入力する。削除制御プログラム113が起動され、クライアント100から入力された削除するデータがこれに渡される。削除制御プログラム113は、削除するデータをデータ探索プログラム114に渡す。データ探索プログラム114は、検索条件作成プログラム115により削除するデータを暗号化し、検索実行プログラム116により削除するデータのシリアル番号を取り出し、削除制御プログラム113に渡す。削除制御プログラム113は、前記シリアル番号を削除条件作成プログラム126に渡す。削除条件作成プログラム126は、渡されたデータから管理テーブル107と鍵テーブル108のためのSQL文をそれぞれ作

成し、それを削除制御プログラム113に渡す。削除制御プログラム113は、削除条件作成プログラム126で作成したSQL文を削除実行プログラム127に渡す。削除実行プログラム127は、データベース管理プログラム110を使って管理テーブル107と鍵テーブル108から渡されたシリアル番号の行を削除する。

【0031】上述の処理をフローチャートを用いて、さらに詳細に説明する。以下の説明では、具体例として図2の管理テーブルと図3の鍵テーブルを用いた場合について説明する。図8は登録・更新プログラム111が実行する暗号化データベースへのデータの登録処理フローを示している。

【0032】データ登録処理は、登録データ入力ステップ800、登録準備ステップ801、登録データSQL文作成ステップ802およびデータベース登録ステップ803からなる。登録データ入力ステップ800では、ユーザがクライアント100から入力した登録するデータを読み込む。登録準備ステップ801では、シリアル番号を作成し、登録するデータのハッシュ値を計算し、登録するデータを暗号化するデータ暗号鍵を作成し、そのデータ暗号鍵で登録するデータを暗号化する。データ暗号鍵を鍵暗号鍵で暗号化する。登録データSQL文作成ステップ802では、登録準備ステップ801で作成したシリアル番号、計算したハッシュ値、暗号化されたデータ暗号鍵、暗号化された登録するデータから、管理テーブル107と鍵テーブル108に登録するSQL文を作成する。データベース登録ステップ803では、登録実行プログラム123が登録データSQL文作成ステップ802で作成したSQL文を実行して、データベース管理プログラム110により管理テーブル107にシリアル番号と暗号化された登録するデータを登録し、鍵テーブル108にシリアル番号と登録データのハッシュ値と暗号化した登録データを暗号化した鍵と暗号化アルゴリズム識別子を登録する。

【0033】次に、登録準備ステップ801の処理を図9のフローチャートを使って詳細に説明する。登録準備ステップ801は、シリアル番号作成ステップ900、ハッシュ値計算ステップ901、暗号アルゴリズム決定ステップ902、データ暗号化ステップ903および鍵暗号化ステップ904からなる。シリアル番号作成ステップ900では、管理テーブル107と鍵テーブル108のそれぞれの行を関係付けるシリアル番号を作成する。ハッシュ値計算ステップ901では、登録するデータのハッシュ値を計算する。暗号アルゴリズム決定ステップ902では、暗号化プログラム120が今回の暗号化に使用する暗号化アルゴリズムを決定する。暗号化プログラム120は複数の暗号アルゴリズムを持つことができ、その中で登録・更新時の暗号化にはもっとも新しく暗号化プログラム120に登録された暗号アルゴリズムを使用するようにしている。データ暗号化ステップ9

03では、登録するデータを暗号化するためのデータ暗号鍵を作成し、そのデータ暗号鍵で登録するデータを暗号化する。鍵暗号化ステップ904では、データ暗号化ステップ903で作成した鍵を鍵格納エリア128にある鍵暗号鍵を使って暗号化する。

【0034】図10は検索制御プログラム112が実行する暗号化データベースへのデータの検索処理フローを示している。データ検索処理は、検索データ入力ステップ1000、ハッシュ値計算ステップ1001、検索SQL文作成ステップ1002、管理テーブル検索ステップ1003、管理テーブル一致データチェックステップ1004、鍵テーブル検索ステップ1005、鍵テーブル一致データチェックステップ1006、検索結果表示ステップ1007、シリアル番号取得ステップ1008、全データ復号ステップ1009からなる。検索データ入力ステップ1000では、ユーザがクライアント100から入力した検索するデータを読み込む。ハッシュ値計算ステップ1001では、検索するデータのハッシュ値を計算する。検索SQL文作成ステップ1002では、ハッシュ値計算ステップ1001で計算したハッシュ値に一致する行の暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を鍵テーブル108から取り出し（ハッシュ値についてのSQL文を作成して鍵テーブルから取り出す）、データ暗号鍵を復号し、その復号したデータ暗号鍵で検索データを暗号化して、管理テーブルを検索するSQL文を作成する。管理テーブル検索ステップ1003では、検索SQL文作成ステップ1002で作成したSQL文により管理テーブル107を検索する。管理テーブル一致データチェックステップ1004では、検索SQL文作成ステップ1002で作成したSQL文に一致するデータが管理テーブル107にあるかどうか調べる。検索SQL文作成ステップ1002で作成したSQL文に一致するデータが管理テーブル107にある場合、シリアル番号取得ステップ1008に進む。シリアル番号取得ステップ1008では、管理テーブル107で一致したデータの鍵テーブル108のシリアル番号を取り出す。全データ復号ステップ1009では、シリアル番号取得ステップ1008で取り出したシリアル番号からすべての暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を取り出し、鍵暗号鍵で復号したデータ暗号鍵と、暗号化アルゴリズムにより管理テーブルの暗号化されたデータをすべて復号化する。管理テーブル検索ステップ1003に戻り処理を続ける。

【0035】検索SQL文作成ステップ1002で作成したSQL文に一致するデータが管理テーブル107にない場合、鍵テーブル検索ステップ1005に進み、鍵テーブル108を検索し、ハッシュ値計算ステップ1001で計算したハッシュ値に一致する行がまだあるか調べる。鍵テーブル一致データチェックステップ1006では、鍵テーブル検索ステップ1005の検索結果を判

定する。ハッシュ値計算ステップ1001で計算したハッシュ値に一致する行がある場合、検索SQL文作成ステップ1002に戻り、新たなデータ暗号鍵を使って検索処理を行う。ハッシュ値計算ステップ1001で計算したハッシュ値に一致する行がない場合、検索結果表示ステップ1007に進む。検索結果表示ステップ1007では、クライアントの画面に検索結果が表示される。

【0036】次に、検索SQL文作成ステップ1002の処理を図11のフローチャートを使って詳細に説明する。検索SQL文作成ステップ1002は、暗号化情報取得ステップ1100および暗号化検索データ作成ステップ1101からなる。暗号化情報取得ステップ1100では、鍵テーブル108を検索して、ハッシュ値計算ステップ1001で計算したハッシュ値に一致する行の暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を取り出し、暗号化されたデータ暗号鍵を鍵暗号鍵で復号する。暗号化検索データ作成ステップ1101では、復号したデータ暗号鍵と、暗号化アルゴリズムにより検索条件を暗号化する。

【0037】暗号化されているデータベースを検索する方法として、暗号化された管理テーブルからデータの一つずつ取り出し、それを復号しながら検索条件に一致するかどうかを調べる方法と検索条件をあらかじめ暗号鍵で暗号化しておき、その暗号化した検索条件で暗号化された管理テーブルを検索する方法がある。前者の方法では、管理テーブルからのデータの取り出しごとに復号の処理が発生するため、データベースの検索性能を大きく悪化させる。後者の方法では、検索条件を暗号化する処理が一回発生する以外は、暗号化されていないデータベースとはほぼおなじ検索性能を出すことができる。このため、暗号化された管理テーブルの検索の実現には、後者の方法が性能的に優れている。本実施例においては、後者の方式について説明した。

【0038】本発明の方式のデータ構造では特定のデータ集合ごとに暗号化に使用する鍵が異なるため、鍵テーブル108から検索条件を暗号化する鍵を取り出す手段としてデータのハッシュ値を利用して鍵テーブル108からデータ暗号鍵を検索するようにした。

【0039】図12は登録・更新制御プログラム111が実行する暗号化データベースへのデータの更新処理フローを示している。データ更新処理は、更新データ入力ステップ1200、更新前データ探索ステップ1201、一致データチェックステップ1202、シリアル番号取得ステップ1203、更新後データ暗号化ステップ1204、更新SQL文作成ステップ1205およびデータベース登録ステップ1206からなる。更新データ入力ステップ1200では、ユーザがクライアント100から入力した更新前のデータと更新後のデータを読み込む。更新前データ探索ステップ1201では、更新前のデータを管理テーブル107から検索する。一致デ

タチェックステップ1202では、更新前データ探索ステップ1201で検索した結果を判定する。更新前データ探索ステップ1201で検索した更新前データが管理テーブル107にない場合、更新処理を終了する。

【0040】更新前データ探索ステップ1201で検索した更新前データが管理テーブル107にある場合、シリアル番号取得ステップ1203に進む。シリアル番号取得ステップでは、更新前データ探索ステップ1201で検索した更新前データのシリアル番号を取得する。更新後データ暗号化ステップ1204では、更新後のデータのハッシュ値を計算した後、更新後のデータをデータ暗号鍵で暗号化する。データ暗号鍵を鍵暗号鍵で暗号化する。更新SQL文作成ステップ1205では、シリアル番号取得ステップ1203で取得したシリアル番号と更新後データ暗号化ステップ1204で作成した暗号化した更新後のデータを使って、更新するデータのSQL文を作成する。データベース登録ステップ1206では、データベース管理プログラム110により管理テーブル107のデータを更新実行プログラム124が更新データSQL文作成ステップ1205で作成したSQL文を実行して更新し、鍵テーブル108の更新後のデータのハッシュ値と暗号化したデータ暗号鍵と、暗号化アルゴリズム識別子を更新する。

【0041】次に、更新前データ探索ステップ1201の処理を図13のフローチャートを使って詳細に説明する。更新前データ探索ステップ1201は、ハッシュ値計算ステップ1300、暗号化検索条件作成ステップ1301、管理テーブル検索ステップ1302、および一致データチェックステップ1303からなる。ハッシュ値計算ステップ1300では、検索条件作成プログラム115を起動し、更新前データのハッシュ値を計算する。暗号化検索条件作成ステップ1301では、検索条件作成プログラム115を起動して、鍵テーブル108を検索してハッシュ値に一致する暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を取り出す。鍵暗号鍵でデータ暗号鍵を復号し、復号したデータ暗号鍵と、暗号化アルゴリズム116で検索条件を暗号化する。管理テーブル検索ステップ1302では、検索実行プログラムを起動し、暗号化検索条件作成ステップ1301で暗号化したSQL文で管理テーブル107を検索する。一致データチェックステップ1303では、管理テーブル107に暗号化検索条件作成ステップ1301で作成したSQL文の検索条件に一致するデータがあるかどうかを調べる。暗号化検索条件作成ステップ1301で作成したSQL文の検索条件に一致するデータがある場合は、終了する。

【0042】暗号化検索条件作成ステップ1301で作成したSQL文の検索条件に一致するデータがない場合は、ハッシュ値に一致する別の暗号化されたデータ暗号鍵と暗号化アルゴリズム識別子を取り出す。暗号化され

たデータ暗号鍵を鍵暗号鍵で復号し、復号したデータ暗号鍵と、前記暗号化アルゴリズム識別子に対応する暗号化アルゴリズムで検索条件を暗号化し、その暗号化した検索条件で再度管理テーブル107を検索する。

【0043】次に、更新後データ暗号化ステップ1204の処理を図14のフローチャートを使って詳細に説明する。更新後データ暗号化ステップ1204は、ハッシュ値計算ステップ1400、暗号アルゴリズム決定ステップ1401、データ暗号化ステップ1402および鍵暗号化ステップ1403からなる。ハッシュ値計算ステップ1400では、更新後のデータのハッシュ値を計算する。暗号アルゴリズム決定ステップ1401では、暗号化プログラム120が今回の暗号化に使用する暗号化アルゴリズムを決定する。暗号化プログラム120は複数の暗号アルゴリズムを持つことができ、その中で登録・更新時の暗号化にはもっとも新しく暗号化プログラム120に登録された暗号アルゴリズムを使用するようにしている。データ暗号ステップ1402では、データ暗号鍵を作成し、管理テーブル107に登録するデータを暗号化する。鍵暗号化ステップ1403では、データ暗号鍵を鍵格納エリア128にある鍵暗号鍵により暗号化する。

【0044】図15は、削除制御プログラム113が実行する暗号化データベースのデータの削除処理フローを示している。データ削除処理は、削除データ入力ステップ1500、削除データ探索ステップ1501、一致データチェックステップ1502、シリアル番号取得ステップ1503、削除SQL文作成ステップ1504およびデータベース削除実行ステップ1505からなる。削除データ入力ステップ1500では、ユーザがクライアント100から入力した削除するデータを読み込む。削除データ探索ステップ1501では、削除データを検索する。一致データチェックステップ1502では、削除データ探索ステップ1501で検索した削除データが管理テーブル107にあるかどうかチェックする。削除データ探索ステップ1501で検索した削除データが管理テーブル107にない場合、削除処理を終了する。

【0045】削除データ探索ステップ1501で検索した削除データが管理テーブル107にある場合、シリアル番号取得ステップ1503に進む。シリアル番号取得ステップ1503では、削除データ探索ステップ1501で検索した削除データのシリアル番号を取得する。削除SQL文作成ステップ1504では、シリアル番号取得ステップ1503で取得したシリアル番号を使って削除SQL文を作成する。データベース削除実行ステップ1505では、削除SQL文作成ステップ1504で作成した削除SQL文を使って管理テーブル107と鍵テーブル108からシリアル番号取得ステップ1503で取得したシリアル番号の行を削除する。削除データ探索ステップ1501に戻り、処理を続ける。

【0046】以上、本実施例の特徴として、管理テーブルとそのテーブルの特定の値の集合（フィールド、行、列など）に関する暗号化のための情報（暗号鍵、暗号化アルゴリズム識別子、データのハッシュ値）をもつ鍵テーブルにより秘密情報を管理することを特徴とするデータベース構造、およびその構成におけるデータの登録処理、検索処理、更新処理、削除処理について説明した。本実施例によれば、前記データベース構造を用いて、データ登録または更新時に暗号鍵を動的に変更し、暗号化のための情報を管理テーブルと別管理することにより、暗号化されたデータベースの安全性を高めることができる。また、管理テーブルの特定の値の集合ごとに異なる暗号化アルゴリズムを使用することが可能となり、さらにデータベース稼動中に暗号鍵および暗号化アルゴリズムの切り替えを動的に行うことも可能である。よって本実施例を適用することにより、十分なデータベースの安全性を確保することができる。

【0047】次に、本発明の第二の実施例について説明する。本実施例は図1に示した第一の実施例と同様の構成をとるが、検索時にもデータ暗号鍵を更新するようにした部分が第一の実施例と異なる。第二の実施例の検索方式について図16を使って説明する。第二の実施例のデータ検索処理は、検索データ入力ステップ1600、ハッシュ値計算ステップ1601、検索SQL文作成ステップ1602、管理テーブル検索ステップ1603、管理テーブル一致データチェックステップ1604、鍵テーブル検索ステップ1605、鍵テーブル一致データチェックステップ1606、検索結果表示ステップ1607、シリアル番号取得ステップ1608、全データ復号ステップ1609、鍵テーブル登録ステップ1610および管理テーブル登録ステップ1611からなる。

【0048】図16の検索データ入力ステップ1600から全データ復号ステップ1609までの処理は、図10の検索データ入力ステップ1000から全データ復号ステップ1009までの処理にそれぞれ対応し、同じ処理を行う。鍵テーブル登録ステップ1610において、検索条件に一致したデータを暗号化するためのデータ暗号鍵を新たに作成し、そのデータ暗号鍵を鍵暗号鍵で暗号化して、シリアル番号、暗号化アルゴリズム識別子とともに鍵テーブル108に登録する。管理テーブル登録ステップ1611において、鍵テーブル登録ステップ1610で作成したデータ暗号鍵を使って検索条件に一致したデータを暗号化して管理テーブル107に登録したあと、管理テーブル検索ステップ1603に戻って管理テーブル107の検索を続ける。

【0049】以上、第二の実施例として、データ登録または更新時だけではなく検索時にも暗号鍵を変更する方式について説明した。本実施例によれば、前記データベース構造を用いて、データ登録、更新または検索時に暗号鍵を動的に変更することにより、第一の実施例のデー

タ登録または更新のときよりも頻繁に暗号鍵を更新するため暗号化されたデータベースの安全性をさらに高めることができる。

【0050】次に、本発明の第三の実施例について説明する。第一の実施例では、新しい暗号化アルゴリズムが追加された場合に直ちにそれを使用していた。本実施例は図1に示した第一の実施例と同様の構成をとるが、暗号化アルゴリズムを上位で指定し、指定された暗号化アルゴリズムで暗号化するようにした部分が第一の実施例と異なる。

【0051】図1を使って本実施例について説明する。データベースに暗号化して格納するデータの登録処理の概略について説明する。ユーザがクライアント100からデータベースに登録するデータを入力し、暗号化アルゴリズム識別子を指定する。登録・更新制御プログラム111が起動され、クライアント100から入力された登録するデータと指定された暗号化アルゴリズム識別子が登録・更新制御プログラム111に渡される。登録・更新制御プログラム111は、登録・更新準備プログラム117に登録するデータと暗号化アルゴリズム識別子を渡す。登録・更新準備プログラム117は、初期条件作成プログラム118によりシリアル番号を作成し、ハッシュ値計算プログラム119により登録するデータのハッシュを計算し、暗号化プログラム120によりクライアント100で指定された暗号化アルゴリズム識別子に基づくデータ暗号鍵を作成して、この鍵を使用して登録するデータを暗号化し、さらにそのデータ暗号鍵を鍵暗号化プログラム121が持っている暗号化アルゴリズムにより鍵格納エリア128にある鍵暗号鍵で暗号化する。

【0052】登録・更新準備プログラム117は、シリアル番号、登録されるデータのハッシュ値、暗号化された登録データ、データ暗号鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、これらのデータを登録・更新条件作成プログラム122に渡す。登録・更新条件作成プログラム122は、渡されたデータから管理テーブル107と鍵テーブル108のためのSQL文をそれぞれ作成し、それを登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、登録・更新条件作成プログラム122で作成したSQL文を登録実行プログラム123に渡す。登録実行プログラム123は、データベース管理プログラム110を使って管理テーブル107に、シリアル番号、暗号化された登録データを登録し、鍵テーブル108に、シリアル番号、登録されるデータのハッシュ値、データ暗号鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録する。

【0053】次に、第三の実施例における、データの更新処理の概略について説明する。ユーザがクライアント

100から更新前のデータ、更新後のデータ、および更新後のデータの暗号化アルゴリズム識別子を指定する。登録・更新制御プログラム111が起動され、クライアント100から入力されたパラメータが登録・更新制御プログラム111に渡される。登録・更新制御プログラム111は、更新前のデータをデータ探索プログラム114に渡す。データ探索プログラム114は、検索条件作成プログラム115により更新前のデータを暗号化し、検索実行プログラムにより更新前のデータのシリアル番号を取り出し、登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、シリアル番号、更新後のデータ、更新後のデータを暗号化する暗号化アルゴリズム識別子を登録・更新準備プログラム117に渡す。

【0054】登録・更新準備プログラム117は、ハッシュ値計算プログラムにより、更新後のデータのハッシュ値を計算し、暗号化プログラム120によりクライアント100で指定された更新後のデータを暗号化する暗号化アルゴリズムに基づくデータ暗号鍵を作成して、更新するデータを暗号化し、さらに鍵暗号化プログラム121が、そのデータ暗号鍵を鍵格納エリア128にある鍵で鍵暗号化プログラム121が持っている暗号化アルゴリズムにより暗号化する。登録・更新準備プログラム117は、更新後のデータのハッシュ値、暗号化されたデータ、暗号化されたデータ暗号鍵、暗号化アルゴリズム識別子を登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、シリアル番号、更新後のデータのハッシュ値、暗号化されたデータ、暗号化されたデータ暗号鍵、暗号化アルゴリズム識別子を登録・更新条件作成プログラム122に渡す。登録・更新条件作成プログラム122は、渡されたデータから管理テーブル107と鍵テーブル108のためのSQL文をそれぞれ作成し、それを登録・更新制御プログラム111に渡す。登録・更新制御プログラム111は、登録・更新条件作成プログラム122で作成したSQL文を更新実行プログラム124に渡す。更新実行プログラム124は、データベース管理プログラム110を使って、管理テーブル107のデータと鍵テーブル108のデータのハッシュ値、暗号化されたデータ暗号鍵、暗号化アルゴリズム識別子を更新する。

【0055】以上で説明したように、第三の実施例によれば、上位アプリケーションが、自由に暗号化アルゴリズムを指定することができ、柔軟に暗号化アルゴリズムを選択することができる。

【0056】以上、本発明の特徴として、管理テーブルとそのテーブルの特定のデータ集合（フィールド、行、列など）に関する暗号化のための情報（暗号鍵、暗号化アルゴリズム識別子、データのハッシュ値）をもつ鍵テーブルにより秘密情報を管理することを特徴とするデータベース構造、その構成における暗号化されたデータの

登録、検索、更新、削除、暗号鍵の動的な更新方法、およびデータベース移動中の暗号化アルゴリズムの切り替え方法について説明した。本発明が用いるデータベース管理システムとしては、リレーショナルデータベースおよびオブジェクト指向データベースのいずれでも実施可能である。

【0057】オブジェクト指向データベースを利用する場合には、鍵テーブル108の定義にオブジェクトを利用することになる。また、鍵テーブル108に、ハッシュアルゴリズムのフィールドを追加して、ハッシュアルゴリズムを暗号化アルゴリズムとともに特定のデータ集合ごとに変更することもできる。

【0058】本発明によれば、前記データベース構造を用いて、暗号鍵を動的に変更し、暗号化のための情報を管理テーブルと別管理することにより、暗号化されたデータベースの安全性を高めることができる。また、特定のデータ集合ごとに新しい暗号化アルゴリズムに変更することが可能となり、データベース移動中に暗号鍵および暗号化アルゴリズムの切り替えを動的に行うことも可能である。よって本発明を適用することにより、十分なデータベースの安全性を確保することができる。さらに将来より強固な暗号化アルゴリズムが発明された場合にも、管理データ暗号用のアルゴリズムを動的により強固な方式に切り替えていくことができる。

【0059】

【発明の効果】本発明によれば、暗号化されたデータベースにおいて、データベース移動中に暗号鍵および暗号化アルゴリズムの切り替えを動的に行うことができ、柔軟性を持つ安全な秘密情報管理データベースを作成することができる。

【図面の簡単な説明】

【図1】本発明のデータベースの秘密情報管理方式の実施の一形態の構成を示す図である。

【図2】フィールドごとに暗号化したデータベースの管理テーブルを説明するための図である。

【図3】フィールドごとに暗号化したデータベースの鍵テーブルを説明するための図である。

【図4】行ごとに暗号化したデータベースの管理テーブルを説明するための図である。

【図5】行ごとに暗号化したデータベースの鍵テーブルを説明するための図である。

【図6】列ごとに暗号化したデータベースの管理テーブルを説明するための図である。

【図7】列ごとに暗号化したデータベースの鍵テーブルを説明するための図である。

【図8】本発明により行われるデータベースのデータ登録の手順を説明するフローチャートである。

【図9】本発明により行われるデータベースのデータ登録時の登録・更新準備プログラムの手順を説明するフローチャートである。



【図10】本発明により行われるデータベースのデータ検索の手順を説明するフローチャートである。

【図11】本発明により行われるデータベースのデータ検索時の検索条件作成プログラムの手順を説明するフローチャートである。

【図12】本発明により行われるデータベースのデータ更新の手順を説明するフローチャートである。

【図13】本発明により行われるデータベースのデータ更新時のデータ探索プログラムの手順を説明するフローチャートである。

【図14】本発明により行われるデータベースのデータ更新時の登録・更新準備プログラムの手順を説明するフローチャートである。

【図15】本発明により行われるデータベースのデータ削除の手順を説明するフローチャートである。

【図16】本発明により行われるデータベースの暗号鍵と暗号化アルゴリズムの変更を伴うデータ検索の手順を説明するフローチャートである。

【符号の説明】

100 クライアント  
101 LAN  
102 LANアダプタ  
103 サーバ  
104 CPU

105 バス  
106 磁気ディスク装置  
107 管理テーブル  
108 鍵テーブル  
109 主メモリ  
110 データベース管理プログラム  
111 登録・更新制御プログラム  
112 検索制御プログラム  
113 削除制御プログラム  
114 データ探索プログラム  
115 検索条件作成プログラム  
116 検索実行プログラム  
117 登録・更新準備プログラム  
118 初期条件作成プログラム  
119 ハッシュ値計算プログラム  
120 暗号化プログラム  
121 鍵暗号化プログラム  
122 登録・更新条件作成プログラム  
123 登録実行プログラム  
124 更新実行プログラム  
125 鍵取得プログラム  
126 削除条件作成プログラム  
127 削除実行プログラム  
128 鍵格納エリア

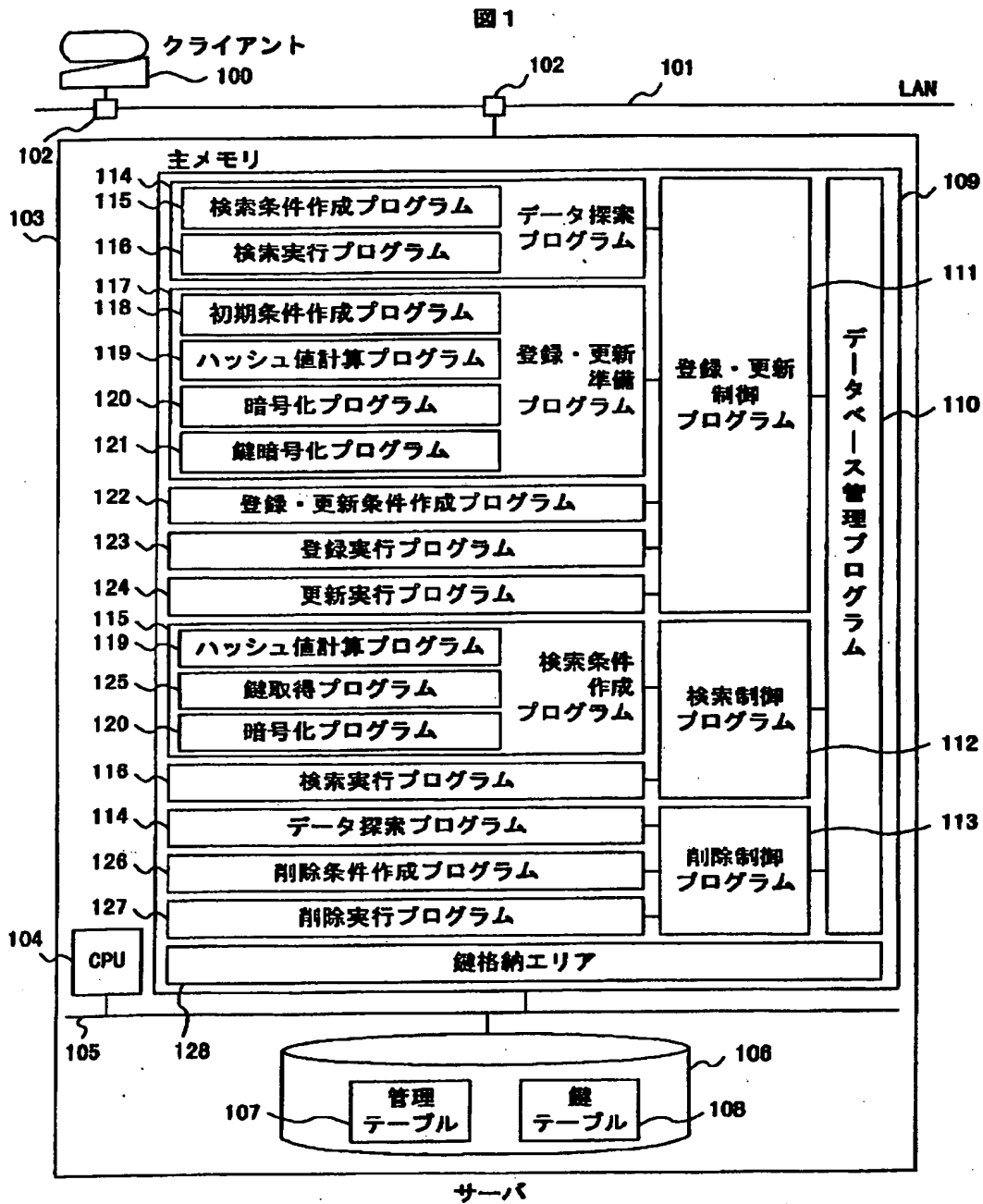
【図2】

図2

	200	201	202	203
	番号	名前	電話番号	住所
204	11	山一平	2222-111	東京都
205	12	山二平	123-4567	神奈川県
206	13	山三平	8765-4321	東京都
	207	208	209	210
	211 管理テーブル			



【図1】



【図3】

図3

番号	名前のハッシュ値	名前暗号アルゴリズム識別子	名前暗号鍵	電話番号ハッシュ値	電話番号暗号アルゴリズム識別子	電話番号暗号鍵	住所ハッシュ値	住所暗号アルゴリズム識別子	住所暗号鍵
11	357	1	225842	156	1	A019MS	123	0	
12	359	1	5158XZ	203	1	882E10	473	0	
13	502	2	3151K8	143	2	123ABD	123	0	

鍵テーブル

【図4】

図4

番号	名前	電話番号	住所
11	日立一郎	111-2222	東京都
12	日立二郎	123-4567	神奈川県
13	日立花子	987-6543	東京都

管理テーブル

【図5】

図5

番号	名前, 電話番号の ハッシュ値	暗号 アルゴリズム 識別子	暗号鍵
11	337	1	24852C
12	459	1	FB24CS
13	532	1	316TK8

鍵テーブル

【図6】

図6

名前	電話番号	住所
宮一平 日	111-2222	東京都
宮二平 日	123-4567	神奈川県
土立花子	987-6543	東京都

管理テーブル

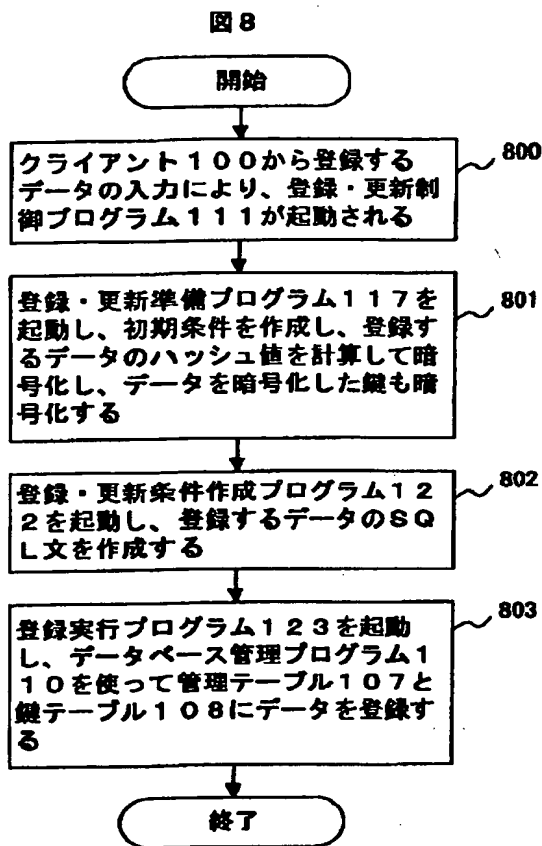
【図7】

図7

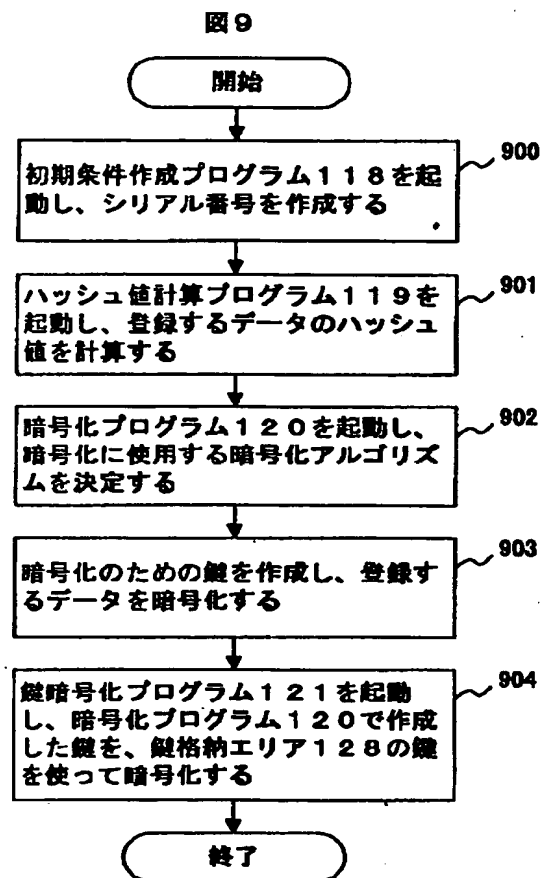
名前 暗号アル ゴリズム識 別子	名前の 暗号鍵	電話番 号暗号 アルゴリ ズム識 別子	電話番号の 暗号鍵	住所 暗号アル ゴリズム識 別子	住所の 暗号鍵
1	24852C	1	5M610V	0	

鍵テーブル

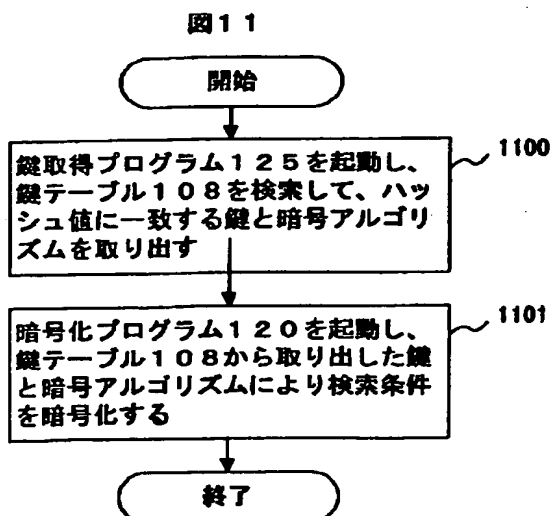
【図8】



【図9】

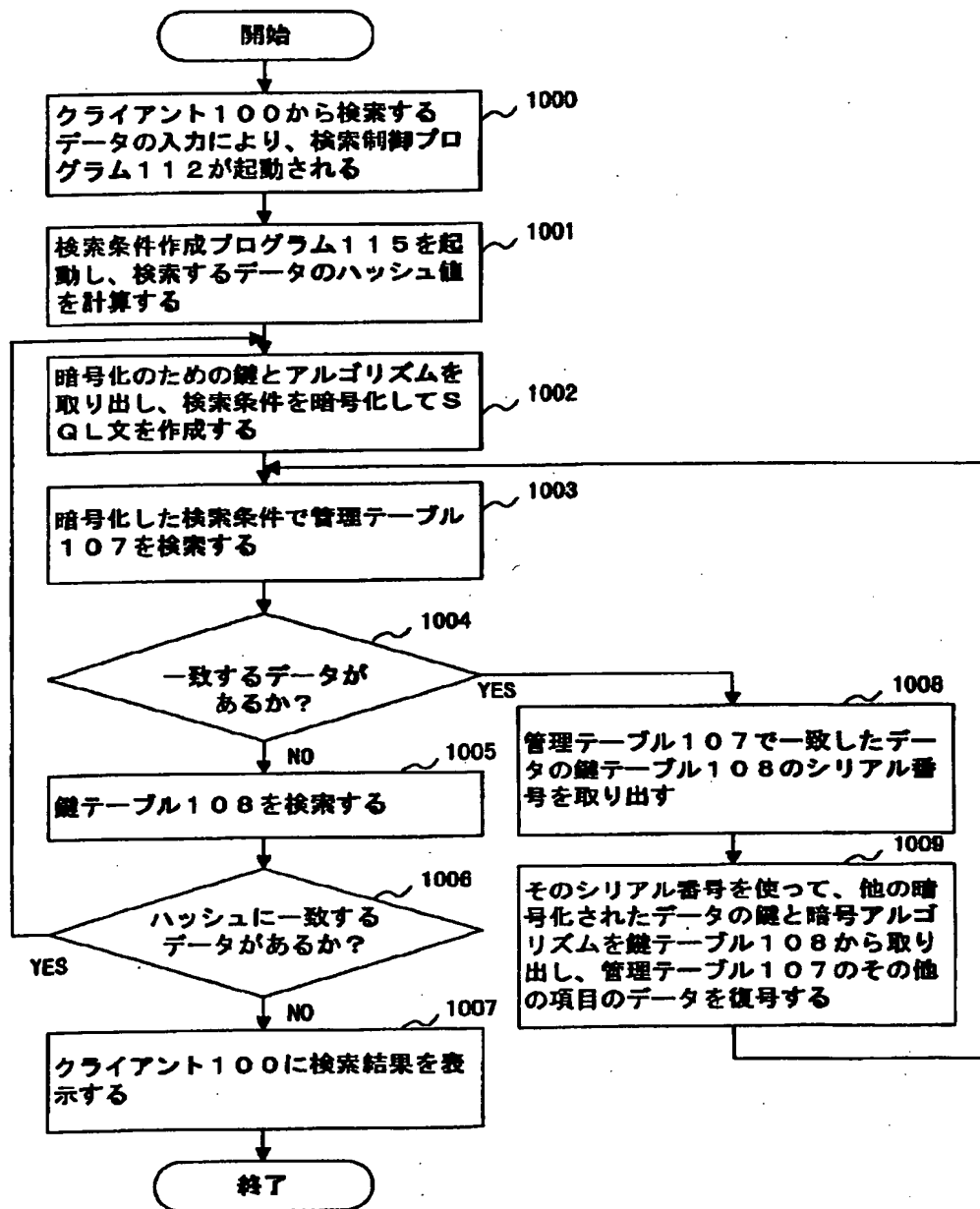


【図11】

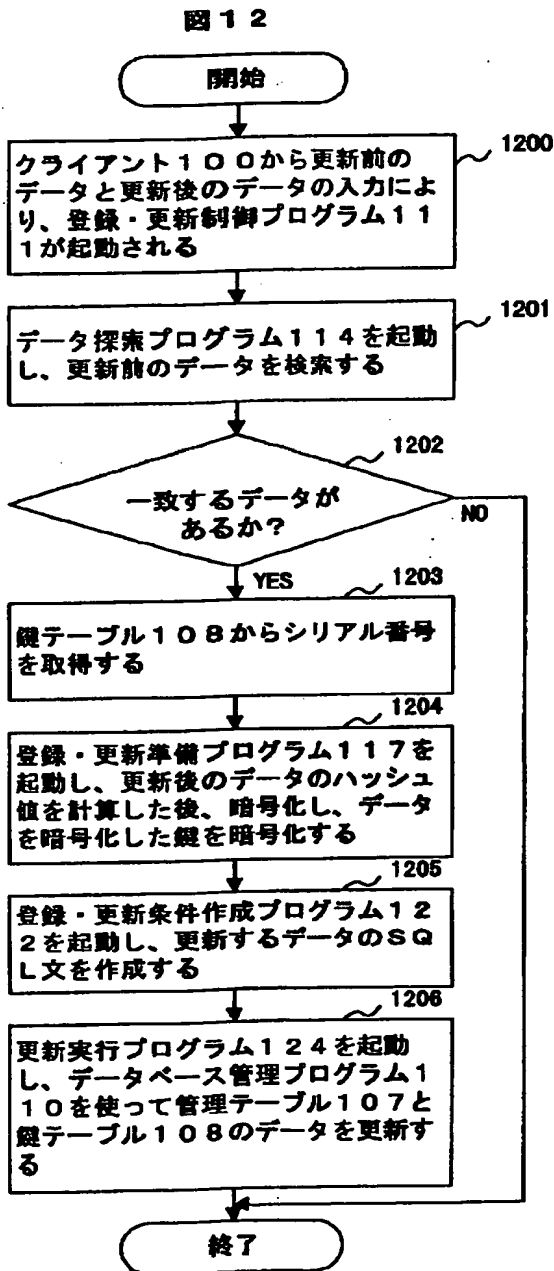


【図10】

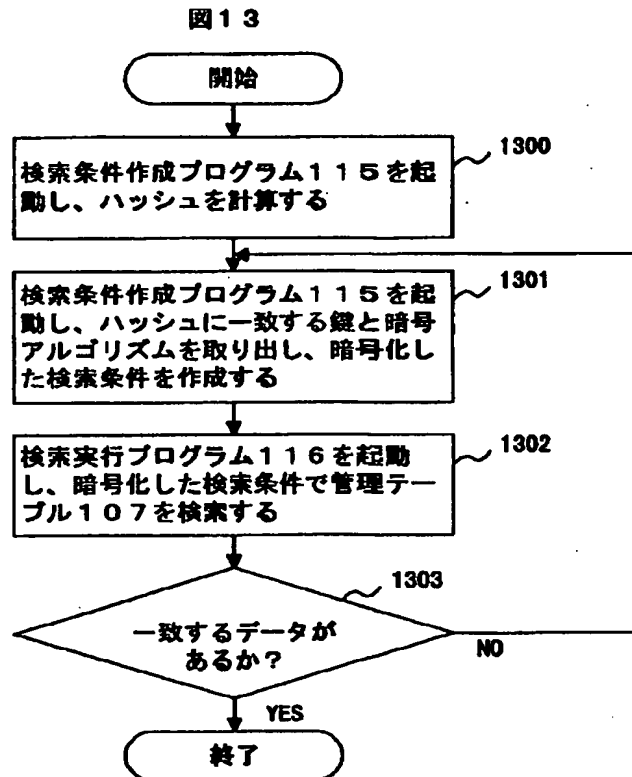
図10



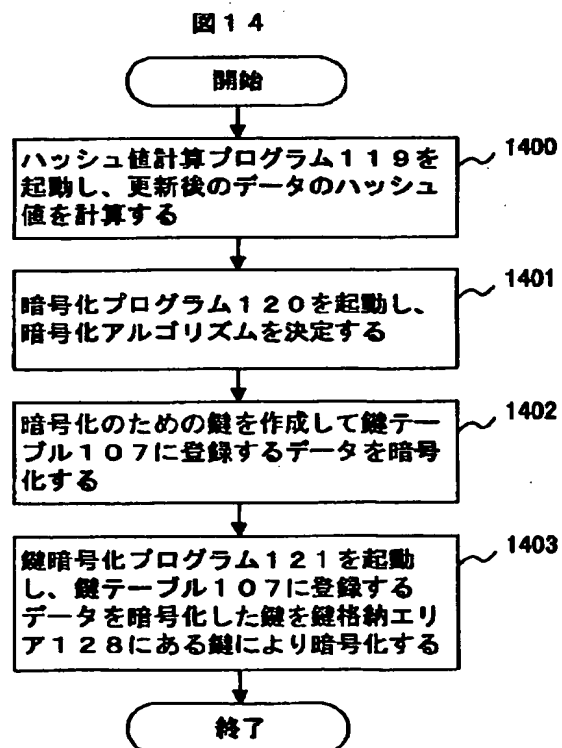
【図12】



【図13】

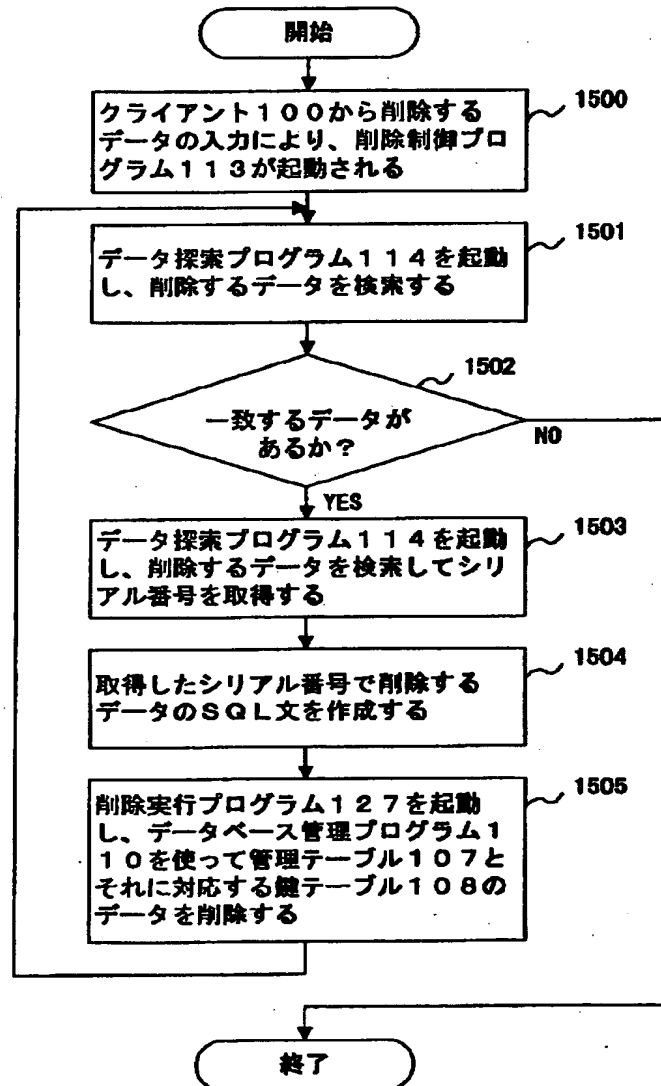


【図14】



【図15】

図15



【図16】

図16

